Amendment To The Claims:

1. (Currently amended) A content processing unit for protecting interchip content pathways transporting digital content objects, the content processing unit comprising:

a first chip package, wherein the first chip package comprises:

a first body,

a first plurality of interconnects,

an encryption engine, and

a first key storage register capable of storing a first key, wherein:

the first key is used by the encryption engine to produce ciphertext content,

the first key storage register is non-readable from outside the first body, and

the first key storage register cannot be overwritten after a programmability period, the programmability period being a period in which the first key is loaded in the first key storage,

a second chip package, wherein the second chip package comprises:

a second body,

a second plurality of interconnects,

a decryption engine, and

a second key storage register capable of storing a second key, wherein:

the second key is used by the decryption engine to produce plaintext content from the ciphertext content, and

the second key storage register is non-readable from outside the second body, the second key storage register being writeable while being non-readable;

a content pathway coupling a ~~first~~ subset of the first plurality of interconnects and a ~~second~~ subset of the second plurality of interconnects, wherein the content pathway transports the digital content objects as the ciphertext content.

2. (Currently amended) The content processing unit for protecting interchip content pathways transporting digital content objects as recited in claim 1, wherein the programmability period ends when a command is sent to the first plurality of interconnects.

3. (Original) The content processing unit for protecting interchip content pathways transporting digital content objects as recited in claim 2, wherein the command activates a fusable link.

4. (Original) The content processing unit for protecting interchip content pathways transporting digital content objects as recited in claim 1, wherein the programmability period ends after writing to the first key storage register.

5. (Original) The content processing unit for protecting interchip content pathways transporting digital content objects as recited in claim 1, wherein at least one of the first and second chip packages comprises a plurality of semiconductor substrates.

6. (Original) The content processing unit for protecting interchip content pathways transporting digital content objects as recited in claim 1, wherein:

the first chip package further comprises a third key storage register capable of storing a key encryption key, and

the first key is protected with the key encryption key outside the first body.

7. (Original) The content processing unit for protecting interchip content pathways transporting digital content objects as recited in claim 1, wherein the second key storage register is overwritable by manipulating the second plurality.

8. (Original) The content processing unit for protecting interchip content pathways transporting digital content objects as recited in claim 1, wherein:

the second chip package further comprises a second encryption engine, and

the second encryption engine uses the second key or another key that is a function of the second key.

9. (Original) The content processing unit for protecting interchip content pathways transporting digital content objects as recited in claim 8, further comprising a third

chip package comprising a third key that can decrypt ciphertext produced with the second encryption engine.

10. (Original) The content processing unit for protecting interchip content pathways transporting digital content objects as recited in claim 1, wherein:

the content processing unit is part of a larger system comprising a third plurality of functionally equivalent content processing units, and

each of the third plurality uses a different first key to protect their respective content pathways.

11. (Currently amended) A method for protecting interchip content pathways transporting digital content objects within a content processing unit, the method comprising steps of:

loading a first key into a first key storage register in a first chip package, wherein the first key in the first key storage register is non-readable from outside the first chip package;

activating a feature of the first chip package that prevents overwriting the first key in the first key storage register from outside the first chip package, after a period in which the first key is loaded in the first key storage;

encrypting digital content with the first key to produce ciphertext content;

coupling the ciphertext content from the first chip package to a content pathway;

loading a second key into a second key storage register in a second chip package, wherein the second key in the second key storage register is non-readable from outside the second chip package, the second key storage register being writeable while being non-readable;

coupling the ciphertext content from the content pathway to a second chip package; and

decrypting the ciphertext content with the second key to reformulate the digital content.

12. (Original) The method for protecting interchip content pathways transporting digital content objects within the content processing unit as recited in claim 11, further comprising steps of:

loading a key encryption key into a third key storage register in the first chip package; and

decrypting the first key with the key encryption key, whereby the first key is protected with the key encryption key outside the first chip package.

13. (Original) The method for protecting interchip content pathways transporting digital content objects within the content processing unit as recited in claim 11, further comprising a step of overwriting the second key in the second key storage register from outside the second chip package.

14. (Original) The method for protecting interchip content pathways transporting digital content objects within the content processing unit as recited in claim 11, further comprising steps of:

encrypting the digital content in the second chip package to produce second ciphertext content using the second key or another key that is a function of the second key,

coupling the second ciphertext content to a second content pathway.

15. (Original) The method for protecting interchip content pathways transporting digital content objects within the content processing unit as recited in claim 11, wherein:

the content processing unit is part of a larger system comprising a plurality of functionally equivalent content processing units, and

each of the plurality uses a different first key to protect their respective content pathways.

16. (Original) A computer system adapted to perform the computer-implementable method for protecting interchip content pathways transporting digital content objects within the content processing unit of claim 11.

17. (Original) A computer-readable medium having computer-executable instructions for performing the computer-implementable method for protecting interchip content pathways transporting digital content objects within the content processing unit of claim 11.

18. (Currently amended) A content processing unit for protecting interchip content pathways transporting digital content objects, the content processing unit comprising:

a first chip package, wherein the first chip package comprises:

a first body,

a first plurality of interconnects,

an encryption engine, and

a first key storage register capable of storing a first key, wherein:

the first key is used by the encryption engine to produce ciphertext content,

the first key storage register is non-readable from the first plurality of interconnects, and

the first key storage register cannot be overwritten after being written once after a period in which the first key is loaded in the first key storage;

a second chip package, wherein the second chip package comprises:

a second body,

a second plurality of interconnects,

a decryption engine, and

a second key storage register capable of storing a second key, wherein:

the second key is used by the decryption engine to produce plaintext content from the ciphertext content, and

the second key storage register is non-readable from the second plurality of interconnects, the second key storage register being writeable while being non-readable;

a content pathway coupling a ~~first~~ subset of the first plurality of interconnects and a ~~second~~ subset of the second plurality of interconnects, wherein the content pathway transports the digital content objects as the ciphertext content.

19. (Original) The content processing unit for protecting interchip content pathways transporting digital content objects as recited in claim 18, wherein:

the first key storage register has a third plurality of bits, and
each of the third plurality can only be written once.

20. (Original) The content processing unit for protecting interchip content pathways transporting digital content objects as recited in claim 18, wherein:
the first chip package further comprises a third key storage register capable of storing a key encryption key, and
the first key is protected with the key encryption key outside the first body.

21. (Original) The content processing unit for protecting interchip content pathways transporting digital content objects as recited in claim 18, wherein the second key storage register is overwritable from outside the second chip package.

22. (Original) The content processing unit for protecting interchip content pathways transporting digital content objects as recited in claim 18, wherein:
the second chip package further comprises a second encryption engine, and
the second encryption engine uses the second key or another key that is a function of the second key.

23. (Original) The content processing unit for protecting interchip content pathways transporting digital content objects as recited in claim 18, wherein:
the content processing unit is part of a larger system comprising a third plurality of functionally equivalent content processing units, and
each of the third plurality uses a different first key to protect their respective content pathways.